UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,471	01/22/2004	Daniel G. Wing	2705-320	6671

20575 7590 07/18/2006

MARGER JOHNSON & MCCOLLOM, P.C.
210 SW MORRISON STREET, SUITE 400
PORTLAND, OR 97204

EXAMINER	
GEE, JASON KAI YIN	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 07/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/763,471	WING, DANIEL G.	
	Examiner	Art Unit	
	Jason K. Gee	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 January 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is response to communication: filed on 01/22/2004.

2. Claims 1-19 are currently pending in this application. Claims 1, 10, and 17 are independent claims.

3. No IDS was received for this application.

Drawings

The drawings are objected to because the pictures are not formal. The Figures provided are all hand-drawn. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because of the hand-written drawings. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 4-7, 12, and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 4 and 5 recite the limitation "the packet switched network." There is insufficient antecedent basis for this limitation in the claim.

Claim 5 recites the limitation "the identified egress devices." There is insufficient antecedent basis for this limitation in the claim.

Claim 6 recites the limitation "the identified non-supporting egress devices." There is insufficient antecedent basis for this limitation in the claim.

Claim 7 recites the limitation "the packet switched network." There is insufficient antecedent basis for this limitation in the claim.

As per claim 12, it is unclear why a second codec with a higher compression is needed with encrypted packets that are not decrypted. The limitations of the previous claim (claim 10) cites that the encrypted IP packet is not decrypted in transport between the packet and circuit switched network. Therefore, all packets should be not decrypted; it is unclear why a second codec would be needed.

As per claim 15, the phrase "the encrypted key" is unclear, as it is not cited whether this is the first or second encrypted key.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-3 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Focsaneanu et al. US Patent No. 5,991,292 (hereinafter '292).

As per claim 1, Focsaneanu '292 teaches a method of transporting encrypted media, comprising: receiving a request (col. 6 lines 18-27 and Figure 5) to transport encrypted (col. 16 lines 1-17) Internet Protocol (IP) media packets over a circuit switched network (Figure 5); establishing an IP link over the circuit switched network (col. 7 lines 29-67); and transporting the encrypted IP media packets over the IP link established over the circuit switched network (Figure 5, where packets are transferred from the terminals to the PSTN).

As per claim 2, Focsaneanu '292 teaches establishing a data channel over the circuit switched network and using a Point to Point Protocol over the data channel to establish the IP link (col. 16 lines 1-17).

As per claim 3, Focsaneanu '292 teaches establishing a data channel over an ISDN channel of a Public Services Telephone Network (col. 16 lines 1-17 and also Figures 16 and 17).

8. Claims 1-3, 5, and 17 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by voit et al. US Patent No. 6,137,869 (hereinafter '137).

As per claim 1, Voit '869 teaches a method of transporting encrypted media, comprising: receiving a request to transport encrypted Internet Protocol (IP) media packets over a circuit switched network (col. 5 lines 48-62, Figure 1B); establishing an IP link over the circuit switched network (Figure 1B, col. 10 lines 59-64); and transporting the encrypted IP media packets over the IP link established over the circuit switched network (col. 5 lines 47-61, col. 10 lines 59-64, and also inherent that these packets are sent through the established IP link).

As per claim 2, 'Voit '869 teaches establishing a data channel over the circuit switched network and using a PPP over the data channel to establish the link (col. 10 lines 59-64).

As per claim 3, Voit '869 teaches establishing the data channel over an ISDN channel of a PSTN (col. 14 lines 30-37).

As per claim 5, Voit '869 teaches receiving call requests from endpoints connected to the packet switched network (Figure 1B, showing connections with the packet and circuit switched network with ITG 118, and Figure 2 showing the details of the connections, described in col. 9 lines 11-53); identifying the call requests that require IP encryption (inherent has it identifies all call requests, and encryption is shown in col. 9 lines 35-53); identifying ingress devices in the circuit switched network associated with the identified call requests that support transport of the encrypted IP media packets over the circuit switched network (col. 9 lines 35-53); establishing IP links over the circuit switched network with the identified egress devices (col. 10 lines 60-65); and transporting the encrypted IP media packets to the identified ingress

devices (inherent and taught throughout the reference, as the ingress devices are connected to the Internet and packets are exchanged during communications after they are connected; col. 9 line 35 to col. 10 line 40).

Independent claim 17 is rejected using the same basis of arguments used to reject claims 1, 2, 3, and 5 above, as all the elements contained in claim 17 are included in claims 1, 2, 3, and 5.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 4, 10, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Voit '869 as applied above, and in view of Edgett et al. US Patent Application Publication 2003/0056092 (hereinafter '092).

As per claim 4, Voit '869 does not explicitly teach including transporting the encrypted IP media packets over the packet switched network without decrypting or decoding the media in the encrypted IP media packets. However, this is taught in Edgett '092. As can be seen in Figure 2 and paragraphs 65 and 66, the encrypted

media packets are sent through the packet switched network and are decrypted only after It passes through the packet switched network into the network decryption server.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include sending packets over a packet switched network without decrypting or decoding the media. One of ordinary skill in the art would have been motivated to perform such an addition to increase security by not sending out critical information which is unencrypted. This is taught in '092 in paragraph 13-16, where it teaches that this invention wants to improve on the ability to send out critical information in packets which is encrypted.

As per independent claim 10, Voit '869 teaches a network processing device, comprising: a processor configured to establish a connection between two endpoints that extends over an Internet Protocol (IP) network and a circuit switched network (Figure 1B), the processor forwarding packets having an encrypted IP packet payload between the two endpoints (col. 5 lines 48-61). However, Voit does not explicitly teach wherein the packet payload is not decrypted when transferred between the IP network and circuit switched network. However, this is taught in Edgett '092. As can be seen in Figure 2 and paragraphs 65 and 66, the encrypted media packets are sent through the packet switched network and are decrypted only after it passes through the packet switched network into the network decryption server. These packets are not decrypted between the packet and circuit switched communication.

As per claim 11, 'Voit '869 teaches wherein the processor establishes an IP link over the circuit switched network and forwards the encrypted IP packet payload over the IP link (col. 10 lines 59-64).

11. Claims 6, 7, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Voit '869 as applied above, and in view of Bulfer et al. US Patent No. 5,392,357 (hereinafter '357).

As per claim 6, Voit '869 teaches all the limitations in the previous claims, but does not explicitly teach the limitations of claim 6. However, Bulfer '357 teaches identifying non-supporting ingress devices in circuit switched network associated with the identified call requests that do not support transport of encrypted IP media packets over the circuit switched network (col. 12 line 23 to col. 13 line 34); establishing circuit switched connections over the circuit switched network for the identified non-supporting egress devices (col. 12 line 23 to col. 13 line 34 where connections are established in order to decode/encode); decrypting and decoding media in the encrypted IP media packets associated with the non-supporting egress devices (col. 12 line 23 to col. 13 line 34); and re-encoding and re-encrypting the media into a circuit switched network format; and transporting the re-encoded and re-encrypted media over the circuit switched connections to the non-supporting egress devices (col. 12 line 23 to col. 13 line 34). (Also, this is all summed up in the summary in (col. 2 lines 5-15, also seen in Figure 1).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include decoding/decrypting media and reencoding/reencrypting in a circuit switched network. One of ordinary skill in the art would have been motivated to perform such an addition to allow flexibility so that different parties may engage in secure communications with one another. This is taught in '357 in col. 1 lines 30-38, where it cites "present security techniques have several limitations, including the general requirement that both the calling and called parties that desire to engage in a secure communication must have compatible security equipment that can send and receive encrypted signals using common handshaking protocols and encryption algorithms. If this is not the case, secure communications are normally not possible." It goes on in col. 2 lines 26-30 to teach "The invention also permits secure communication between parties using security devices with different handshaking protocols and encryption algorithms."

As per claim 7, Voit '869 teaches all the limitations of the previous claims, but does not explicitly teach the specifics of key exchange taught in claim 7. However, this is taught in '357 in col. 12 line 50 to col. 14 line 14. The training mentioned in these passages deal with key exchange, which is taught in col. 8 lines 26-44.

As per claim 18, Voit '869 teaches authenticating the identified call requests with ingress gateways (col. 5 lines 44-61) and conducing PPP sessions with the ingress gateways when the ingress gateways are authenticated (col. 10 lines 60-64). Exchanging encryption keys are taught in Bulfer '357 in col. 8 lines 27-44.

12. Claim 8 is rejected under 35 U.S.C. 103(a) as being obvious over Voit '869.

As per claim 8, Voit '869 teaches encrypting the media packets (col. 5 lines 48-62), but does not explicitly teach encrypting and decrypting the packets only once. However, the Examiner asserts that this would be obvious. One of ordinary skill in the art would have been motivated to encrypt/decrypt packets only once, as it provides security, and it saves time compared to encrypting/decrypting more than once.

13. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Voit '869 as applied above, and in view of Lindholm et al. US Patent Application Publication 2004/0019801 (hereinafter '801).

As per claim 9, Voit '869 teaches the utilizing PPP and ISDN in (col. 10 lines 59-64 and col. 14 lines 30-37), but does not explicitly teach using SRTP. However, this is taught in Lindholm '801 in paragraph 26.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to utilize SRTP. One of ordinary skill in the art would have been motivated to perform such an addition to provide confidentiality and protection of the user. This is taught in paragraph 26, where it cites "An example of such a cryptographic mechanism is the Secure Real-time Transport Protocol (SRTP), which can provide both confidentiality protection of the user data and integrity protection on a per packet basis."

14. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Voit '869 in view of Bulfer '357 as applied above, and further in view of Bruce Schneier's *Applied Cryptography* (2nd Edition).

As per claim 19, the Voit and Bulfer combination teaches all the limitations of the previous claims, but does not explicitly teach encrypting the encryption keys using shared keys and sending the encrypted encryption key to the ingress gateways. However, Schneier teaches encrypting keys using shared keys and sending the encrypted keys out. This is taught on pages 47 and 48.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include encrypted key exchange in a circuit switched network. One of ordinary skill in the art would have been motivated to perform such an addition to allow flexibility so that different parties may engage in secure communications with one another. This is taught in '357 in col. 1 lines 30-38, where it cites "present security techniques have several limitations, including the general requirement that both the calling and called parties that desire to engage in a secure communication must have compatible security equipment that can send and receive encrypted signals using common handshaking protocols and encryption algorithms. If this is not the case, secure communications are normally not possible." It goes on in col. 2 lines 26-30 to teach "The invention also permits secure communication between parties using security devices with different handshaking protocols and encryption algorithms."

15. Claims 4, 10, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 as applied above, and in view of Edgett et al. US Patent Application Publication 2003/0056092 (hereinafter '092).

As per claim 4, Focsaneanu does not explicitly teach including transporting the encrypted IP media packets over the packet switched network without decrypting or decoding the media in the encrypted IP media packets. However, this is taught in Edgett '092. As can be seen in Figure 2 and paragraphs 65 and 66, the encrypted media packets are sent through the packet switched network and are decrypted only after It passes through the packet switched network into the network decryption server.

As per independent claim 10, Focsaneanu teaches a processor configured to establish a connection between two endpoints that extends over an Internet Protocol network and a circuit switched network (Figure 8), the processor forwarding packets having an encrypted IP packet payload between the two endpoints (col. 16 lines 1-17). However, Focsaneanu does not explicitly teach that the encrypted IP packets are not decrypted when transferred between the IP network and circuit switched network. However, this is taught in Edgett '092. As can be seen in Figure 2 and paragraphs 65 and 66, the encrypted media packets are sent through the packet switched network and are decrypted only after it passes through the packet switched network into the network decryption server. These packets are not decrypted between the packet and circuit switched communication.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include sending packets over a packet switched network without decrypting or decoding the media. One of ordinary skill in the art would have been motivated to perform such an addition to increase security by not sending out critical information which is unencrypted. This is taught in '092 in paragraph 13-16, where it teaches that this invention wants to improve on the ability to send out critical information in packets which is encrypted.

As per claim 11, Focsaneanu teaches wherein the processor establishes an IP link over the circuit switched network and forwards the encrypted IP packet payload over the IP link (col. 16 lines 1-17).

16. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 as applied above, and in view of Lindholm et al. US Patent Application Publication 2004/0019801 (hereinafter '801).

As per claim 9, Focsaneanu '292 teaches the utilizing PPP and ISDN in (col. 16 lines 1-17), but does not explicitly teach using SRTP. However, this is taught in Lindholm '801 in paragraph 26.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to utilize SRTP. One of ordinary skill in the art would have been motivated to perform such an addition to provide confidentiality and protection of the user. This is

taught in paragraph 26, where it cites "An example of such a cryptographic mechanism is the Secure Real-time Transport Protocol (SRTP), which can provide both confidentiality protection of the user data and integrity protection on a per packet basis."

17. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 and in view of Edgett '092 as applied above, and further in view of obviousness over Saadat et al. US Patent Application Publication 2005/0125357 (hereinafter '357).

As per claim 12, Focsaneanu teaches the use of Codec, as can be seen in Figures 8 and 14, but the Focsaneanu and Edgett combination does not explicitly teach compressing a non-decrypted data at a higher compression rate using a second codec. However, compressing data at different rates due to encryption or decryption is taught in Saadat in paragraph 80.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to compress data using different codecs. One of ordinary skill in the art would have been motivated to perform such an addition allow more efficiency when storing or transporting material by compressing materials at different compression rates. This is taught in paragraphs 11 and 12, where it teaches that the new invention would overcome the old art by providing a cheaper and better way to store video without lowering video quality.

18. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 and in view of Edgett '092 as applied above, and further in view of Bowman-Amuah US Patent No. 6,426,948 (hereinafter '948).

As per claim 13, the '292 and '092 combination does not explicitly teach identifying phone numbers that can be transferred between the IP network and the circuit switched network without decrypting the encrypted IP packets payload. However, Bowman-Amuah '948 teaches storing up phone numbers in col. 39 lines 20-30.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include a memory containing a dial plan for identifying phone numbers. One of ordinary skill in the art would have been motivated to perform such an addition to allow easy access to those who use the system regularly. This is taught in col. 39 lines 19-22: "For callers that utilize the callback system on a regular basis a custom profile is provided as an extension to the users existing profile information.

19. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 and in view of Edgett '092 as applied above, and further in view of Bruce Schneier's *Applied Cryptography* (2nd Edition).

As per claim 14, '292 and '092 does not explicitly teach receiving a first key from a first endpoint, encrypting the first key using the shared key and sending the encrypted first key to the ingress device. However, this is taught in Schneier on page 48. (Memory for storing a key is inherent as it uses the key).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to incorporate the use of Key Exchange in a secure hybrid system of circuit and packet switched networks. One of ordinary skill in the art would have been motivated to perform such an addition to allow easy security use. This is taught by Schneier on page 48, where it cites "In some practical implementations, both Alice's and Bob's signed public keys will be available on a database. This makes the key-exchange protocol even easier, and Alice can send a secure message to Bob even if he has never heard of her."

20. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 and in view of Edgett '092 and Schneier, and further in view of Bulfer et al US Patent No. 5,392,357 (hereinafter '357).

As per claim 15, the '292 combination does not explicitly teach the limitations of claim 15, but Bulfer teaches this in col. 12 line 50 to col. 14 line 14. The training mentioned in these passages deal with key exchange, which is taught in col. 8 lines 26-44.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include key exchange in a circuit switched network. One of ordinary skill in the art would have been motivated to perform such an addition to allow flexibility so that different parties may engage in secure communications with one another. This is taught in '357 in col. 1 lines 30-38, where it cites "present security techniques have several limitations, including the general requirement that both the calling and called parties that

desire to engage in a secure communication must have compatible security equipment that can send and receive encrypted signals using common handshaking protocols and encryption algorithms. If this is not the case, secure communications are normally not possible." It goes on in col. 2 lines 26-30 to teach "The invention also permits secure communication between parties using security devices with different handshaking protocols and encryption algorithms."

21. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Focsaneanu '292 and in view of Edgett '092 as applied above, and further in view of Lindholm et al. US Patent Application Publication 2004/0019801 (hereinafter '801).

As per claim 16, Focsaneanu '292 teaches the utilizing PPP and ISDN in (col. 16 lines 1-17), but the combination does not explicitly teach using SRTP. However, this is taught in Lindholm '801 in paragraph 26.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to utilize SRTP. One of ordinary skill in the art would have been motivated to perform such an addition to provide confidentiality and protection of the user. This is taught in paragraph 26, where it cites "An example of such a cryptographic mechanism is the Secure Real-time Transport Protocol (SRTP), which can provide both confidentiality protection of the user data and integrity protection on a per packet basis."

Conclusion

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason K. Gee whose telephone number is (571) 272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-38386962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Gee
Patent Examiner
Technology Center 2134
07/08/06

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100